UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL NO. 09-10243-MLW
	)	
RYAN HARRIS	)	

MEMORANDUM IN SUPPORT OF DEFENDANT'S RENEWED MOTION TO DISMISS, AND FOR JUDGMENT OF ACQUITTAL, ON THE GROUNDS OF UNCONSTITUTIONAL VAGUENESS

Defendant, Ryan Harris, respectfully submits this Memorandum in support of his renewed motion to dismiss and for judgment of acquittal because this application of the wire fraud statute is unconstitutionally void for vagueness in violation of his due process rights.

I. THIS APPLICATION OF THE WIRE FRAUD STATUTE IS VOID FOR VAGUENESS AND HARRIS'S CONVICTION IS UNCONSTITUTIONAL

In his motion to dismiss, Harris raised the argument that the wire fraud statute was void for vagueness as applied to his case. At a hearing on the motion to suppress, this Court declined to address the issue, stating that it would need to be revisited after all of the evidence was presented at trial. Tr. 12/13/11 at 65-66. Harris reasserted this issue in his pre-verdict Rule 29 motion. Now that all of the evidence has been presented, this Court should consider Harris's argument that this case should be dismissed because his prosecution is void for vagueness.

The void-for-vagueness doctrine requires that a penal statute define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement. Kolender v. Lawson, 461 U.S. 352, 357 (1983). This doctrine "addresses concerns about (1) fair notice and (2) arbitrary and discriminatory prosecutions." Skilling v. United States, 130 S.Ct. 2896, 2933

(2010); see also Arthur Andersen LLP v. United States, 544 U.S. 696, 704 (2005) ("[A] fair warning should be given to the world in language that the common world will understand of what the law intends to do if a certain line is passed." (internal quotation marks omitted)). The concern here is notice.

Both before and during trial, this Court noted the potential breadth of the wire fraud statute, and held that it could be the basis for liability where even the traditionally broad conspiracy and aiding and abetting statutes did not apply. This potential inherent in the wire fraud statutes has been recognized by courts as well as commentators. See e.g., United States v. Czubinski, 106 F.3d 1069, 1079 (1st Cir. 1997). One commentator described the analogous mail fraud statute as "destined to provide the federal prosecutor with what Archimedes long sought–a simple fulcrum from which one can move the world," and warned that this expansion would "dwarf and trivialize much of the remainder of substantive federal criminal law" as well as circumventing statutory defenses and enhancing prosecutorial power over defendants. John C. Coffee, Jr., The Metastasis of Mail Fraud: The Continuing Story of the 'Evolution' of a White-Collar Crime, 21 Am. Crim. L. Rev. 1, 3 (1983). Cases like Czubinski imply that there are boundaries inherent in these fraud statutes, but leave those boundaries undefined. Additionally, like the mail fraud statute, the wire fraud statute comes very close to punishing solely bad thoughts without accompanying actions. Id. Because wire fraud requires only a scheme to defraud plus a "remotely foreseeable" use of the wires, "the substantive crime of [wire] fraud consist[s] of little more than an evil scheme." Id.

The breadth of the wire fraud statute implicates serious due process concerns. Novel prosecutions such as this one allow the government to avoid the Constitution's prohibition

against ex post facto laws. U.S. Const. art. 1, sec. 9. Congress has passed no law prohibiting cloned modems, and if it did so now, its strictures could not apply to the conduct charged in this case. Yet the elasticity of the wire fraud statute theoretically permits prosecutors to avoid this result and to determine themselves what conduct ought to be prohibited by federal law. Courts have recently warned against prosecutorial attempts " to stretch criminal law beyond its proper bounds":

> This is not the way criminal law is supposed to work. Civil law often covers conduct that falls in a gray area of arguable legality. But criminal law should clearly separate conduct that is criminal from conduct that is legal. This is not only because of the dire consequences of a conviction–including disenfranchisement, incarceration and even deportation–but also because criminal law represents the community's sense of the type of behavior that merits the moral condemnation of society. When prosecutors have to stretch the law or the evidence to secure a conviction, as they did here, it can hardly be said that such moral judgment is warranted.

United States v. Goyal, 629 F.3d 912, 922 (9th Cir. 2010) (C.J. Kozinski, concurring); United States v. Brown, 459 F.3d 509, 523 (5th Cir. 2006) (noting Circuit's "repeated exhortation against expanding federal criminal jurisdiction beyond specific federal statutes to the defining of common-law crimes" in reversing wire fraud conviction based on honest services theory). Not only did Harris not have notice that his conduct was potentially criminal, the result of this case seems to dictate that Harris could be responsible any time someone obtained or used a TCNISO product regardless of how that individual got the product, how he used it, or when he used it. Additionally, the expansion of the wire fraud statute in this case could have wide-reaching implications for technology companies.

A. Similar Technology

This is a case of first impression; apart from Harris's case, the government has not pursued criminal sanctions against individuals who made products with similar capabilities. During proceedings related to Harris's Motion to Dismiss, the government noted three cases involving modified modems. Two of these cases were instituted after Harris's case, and the government brought and then dismissed the third shortly before the Grand Jury returned an indictment in this case.[1] At the time of the alleged conduct, no specific law or case would have indicated to Harris that making and selling modified modems would subject him to federal criminal liability.[2] Contrast this with the recent Megaupload prosecution based on allegations of widespread and purposeful copyright infringement enabled by an internet-based file-sharing service. United States v. Dotcom, et al., C. 12-00003 (E.D.Va.). Multiple civil cases resulting in the termination of file-sharing sites such as Napster and Grokster and hefty settlements against their users because of copyright violations would have given Megaupload notice that running a website that permits such file sharing put it at risk of violating the copyright statutes, which can lead to criminal prosecution.

---

[1] These three cases are: United States v. Robles, Cr. 11-00602 (C.D.Cal.) (defendant pled guilty to a one-count Information charging a misdemeanor violation of unauthorized access to a protected computer in violation of 18 U.S.C. § 1030(a)(2)(c), with the government recommending a term of probation); United States v. Delorey, Cr. 10-00682-JCF (S.D.N.Y.) (defendant pled guilty to a single count information charging a misdemeanor violation of fraudulent access to a protected computer in violation of 18 U.S.C. § 1030(a)(6), and was sentenced to 4 months in custody); United States v. Swingler, 09-033 (S.D.N.Y.) (complaint dismissed on July 20, 2009). The indictment against Harris was returned on August 19, 2009.

[2] Neither the black box nor the blue box cases would have hinted at the criminal liability here. Those cases involved single-use, plug-in devices–black boxes can only be used to obtain free television service, and blue boxes can only be used to make phone calls without paying–quite unlike the multi-purpose tools sold by TCNISO.

Indeed, many products with the same capabilities as TCNISO products exist and have not been and are unlikely to be the subject of a federal criminal prosecution. Contemporary computing platforms and devices, such as Microsoft Windows XP, cell phones, and iPods, automatically detect and connect to unsecured wireless internet networks. These devices are preprogrammed to find any available wireless network, to exploit vulnerable networks, and to permit non-payers to reach and use residential and business networks. MAC addresses are publicly available information, printed on the modems as well as on the boxes in which they are sold. There are free "sniffer" programs available on the internet from major American universities. Mainstream companies like Google sniff MAC addresses and use them to run their geolocation services. There are also websites that permit the anonymous use of the internet. Agent Russell testified that there are no federal prosecutions pending against these sites, but if the verdict in this case stands, one could imagine those prosecutions emerging.

A recent Boston Globe article highlights the serious notice problem present in this case. Just days after it published an article regarding Harris's trial, the Globe published an article about the Tor Project, "[a] Walpole nonprofit company, largely funded by the federal government." Jenifer B. McKim, "Privacy Software, Criminal Use," Boston Globe, March 8, 2012. Tor develops software that permits people to surf the internet anonymously. Id. According to the Tor Project, the product "is designed to help people protect themselves from internet surveillance," and in addition to protecting law enforcement, corporate whistle-blowers, political dissidents, and domestic abuse victims, the software can help users commit crime, including child pornography and drug offenses. Id. The Tor Project's founder said that the company "can't be blamed for aiding crimes in the same way cellphone and computer makers should not be held

accountable for the misuse of those devices," and refuses to develop a way for law enforcement agencies to identify Tor users because it would frustrate his company's purpose. Id. Despite these known illicit uses, the federal government continues to fund Tor–a representative from the National Science Foundation was quoted as saying that "Any technology can be used for ill. . . . It is not a reason not to fund the science." Id. Not once does the article mention the possibility of criminal charges against Tor based on the conduct of its users. In fact, the head of the FBI Cyber Criminal Squad in Boston told the Globe that Tor would make investigations more complex but not impossible, without suggesting that Tor might itself be under investigation. Id.

As for technology products which can test or compromise security systems one might look at a widely used software, Metasploit, distributed by a Boston-based company. In a book describing the software, Metasploit: The Penetration Tester's Guide published by No Starch Press which also offered Harris's book,[3] the author explains that Metasploit can be used to:

- Find exploits in unmaintained, misconfigured, and unpatched systems
- Perform reconnaissance and find valuable information about a target
- Bypass antivirus technologies and circumvent security controls ...
- Use the Meterpreter shell to launch attacks from inside a network.

No Starch Press, Review of Metasploit: The Penetration Tester's Guide, available at http://nostarch.com/releases/metasploit_pr.html. The firmware permits users to "secure their own network or to put someone else's to the test," that is, to hack into secured networks. Id. Computer attackers rely on tools such as Metasploit (and CORE IMPACT and Immunity

[3] No Starch Press publishes books focused on "open source, security, hacking, programming, alternative operating systems." See http://www.nostarch.com.

CANVAS)[4] as powerful aids for launching network attacks. With such tools, an attacker does not have to create custom exploit code or scour the Internet to find code to exploit a hole. In an interview, HD Moore, the creator of Metasploit, acknowledged that Metasploit could help "the bad guys do bad things," but stated that "[t]he value provided by making the software available to everyone outweighs any damage caused by the minority that uses the software to illegally access computer systems. Federico Biancuzzi, Metasploit 3.0 Day, SecurityFocus, Mar. 27. 2007, available at http://www.securityfocus.com/columnists/439.

Unlike Harris, who published a book and software exposing exploits regarding cable service and increased cable speed, Moore did far more: he created "the Swiss army knife used by hackers," see "Students Delve Into Metasploit," May 16, 2011, available at http://blog.uml.edu/cs/2011/05/fu_metasploit_presentations.html, a tool at the core of computer hacks world-wide with more than one million downloads yearly. See "Learn More about the Metasploit Project," available at http://metasploit.com/learn-more/. The Metasploit software is accompanied by a blog, http://feeds.feedburner.com/metasploit/blog,which provides customer support and tutorials. The software is owned, and the blog is maintained, by Rapid7, a Boston-based security company which also owns "John the Ripper," a popular password cracking tool. Rapid7 maintains, as did Harris, that its tools are to be used for security testing only, not for illegal hacking activity. Metasploit, "Penetration Testing Basics," available at

[4]See, e.g., www.coreserurity.com ("By replicating actual threats across the enterprise, our solutions reveal where and how attacks can access your most important information."); www.immunityinc.com (which "makes available hundreds of exploits"). Each of these firms trumpets its security advantages to legitimize its activities. One might cynically characterize the marketing approach as a wide-spread broadcast of the latest hacking innovations to stimulate sales of its anti-hacking products.

http://www.metasploit.com/learn-more/penetration-testing-basics/ ("Let's make one thing crystal clear: Penetration testing requires that you get permission from the person who owns the system. Otherwise, you would be hacking the system, which is illegal in most countries – and trust me, you don't look good in an orange jump suit.").

Apart from the disclaimer, the Metasploit firmware serves a public purpose, to expose vulnerabilities in systems. Harris affirms a similar purpose, saying that "[c]able networks around the world are often misconfigured and highly vulnerable, and this book will expose countless exploits and hacking techniques . . . [providing] a wake-up call for every cable operator to implement all of the DOCSIS security features." Harris, Hacking the Cable Modem at xxiv. Like the founder of the Tor Project, the creator of Metasploit has stated that he is concerned that government regulation of his product would stifle innovation: "I do what I can to prevent [legal regulation of exploits] from coming to pass in the United States, by donating to the [Electronic Freedom Frontier] and trying to make a strong case for the usefulness of exploit code. In the US, exploit regulation would kill research and lead to a degrading state of security for all US companies." Federico Biancuzzi, Metasploit 3.0 Day, SecurityFocus, Mar. 27. 2007, available at http://www.securityfocus.com/columnists/439.

In a world where companies like Tor not only exist, but are supported by government funds, where Rapid7 sells a tool that is as useful for hacking as it is for preventing hacking, where Microsoft makes devices capable of stealing wireless internet, and Google collects MAC addresses to run a geolocation system, absent a specific statute or some prior prosecutions, Harris did not have notice that his conduct violated the federal wire fraud statute.

The Court's instructions offer no way to distinguish between these companies and products and TCNISO and its products. In fact, applying the Court's instructions to many mainstream computer technologies results in the conclusion that many well-known companies are committing wire fraud. The Court's instructions explained that while the sale of a product with known illicit applications does not suffice to establish wire fraud, the nature of the product and the manufacturer's knowledge of the known illicit uses can be considered. Using this rubric, the following companies are likely committing wire fraud:

- Rapid7: The above quotations indicate that the creator of Metasploit knows that his product can be and is used by illicit hackers. Whether he knows the names of the hackers or their illegal objectives appears–in light of Harris's conviction–immaterial.
- Tor Project (and the federal government agencies that fund it): The above quotations indicate that the founder of the Project knows that his product can be and is used to shield criminal activity. Again, knowledge of the aims and names of illicit users appears immaterial.
- Microsoft/Apple: Both companies make devices capable of detecting and connecting to unsecured wireless networks.

B. Civil Proceedings

Computers and the internet present the courts with an ever evolving frontier, and it is the courts who must determine how these new technologies sit within federal laws written at a time when such technology was inconceivable. Generally, the boundaries of the law and in the internet age have been contested in civil proceedings. From Google, to Apple, to Grokster, the

internet behavior of companies has been challenged civilly, not criminally, and not at the price of any person's freedom.

In general, a seller of a product cannot be held civilly liable in connection with the conduct of third party product users. The logic is that "[u]sually the criminal use of a product is deemed to be a supervening, intervening event that eliminates any responsibility on the part of the manufacturer." George A. Nation, Respondeat Manufacturer, 60 Baylor L. Rev. 155, 157-58 (2008); see Delahanty v. Hinckley, 564 A.2d 758, 762 (D.C. Ct. App. 1989) ("'In general no liability exists in tort for harm resulting from the criminal acts of third parties, although liability for such harm sometimes may be imposed on the basis of some special relationship between the parties.'" (quoting Hall v. Ford Enterprises, Ltd., 445 A.2d 610, 611 (D.C. Ct. App. 1982))). Nor do the civil courts typically find liability based on the decision to sell or market a product that can be used for unlawful purposes. See id. at 761; Perkins v. F.I.E. Corp., 762 F.2d 1250, 1265 n.43 (5th Cir. 1985) ("The marketing of a handgun is not dangerous in and of itself, and when injury occurs, it is not the direct result of the sale itself, but rather the result of actions taken by a third party."); McCarthy v. Olin Corp., 119 F.3d 148, 157 (2nd Cir. 1997) (dismissing civil suit filed by crime victims against maker of hollow point bullets and noting that manufacturer "was under no legal duty to prevent criminal misuse of its product").

The idea that intervening criminal conduct by a user prevents civil liability for the manufacturer is long-established. Oliver Wendell Holmes confronted the question "why is not a man who sells fire-arms answerable for assaults committed with pistols bought of him, since he must be taken to know the probability that, sooner or later, some one will buy a pistol of him for some unlawful end?" Holmes, Privilege, Malice, and Intent, 8 Harv. L. Rev. 1, 10 (1894).

Holmes explained that generally, such vicarious liability does not exist, even in civil cases, because "every one has a right to rely upon his fellow-men acting lawfully, and, therefore, is not answerable for himself acting upon the assumption that they will do so, however improbable it may be." Id. (emphasis added).[5]

Courts have been extremely circumspect about extending civil liability past this boundary. An exception is Rice v. Paladin Enterprises, Inc., 128 F.3d 233 (4th Cir. 1997), where the Fourth Circuit determined that a publisher of book entitled Hit Man: A Technical Manual for Independent Contractors could be held civilly liability for aiding and abetting criminal conduct where "a reasonable jury clearly could conclude from the stipulations of the parties, and, apart from the stipulations, from the text of Hit Man itself and the other facts of record, that [the publisher] aided and abetted in Perry's triple murder by providing detailed instructions on the techniques of murder and murder for hire with the specific intent of aiding and abetting the commission of these violent crimes. Id. at 255 (emphasis added). It is notable that the Fourth Circuit reached this conclusion only after determining that the publisher had specific intent to aid

[5] Holmes went on to state the following rule: "[W]here it is sought to make a man answerable for damage, and the act of a third person is nearer in time than the defendant's to the harm, if the third person's act was lawful, it stands like the workings of nature, and the question is whether it reasonably was to be anticipated or looked out for; but if the third person's act was unlawful, the defendant must be shown to have intended the act, or at least to have expected it, and to have intended consequences which could not happen without the act." Holmes, Privilege, Malice, and Intent, 8 Harv. L. Rev. at 11-12. Even assuming that this weaker formulation of the rule is correct and proof of expectation of the unlawful act can form the basis for liability, Holmes was confronting the extent of civil liability, not the potential reach of criminal culpability. There are indications, however, that mere expectation of criminal misconduct cannot form the basis for civil liability. In a related context, Prosser & Keeton explained that "Where there is a malicious or criminal act, the original actor might be free to say, even if anticipating the misconduct, that it was not the actor's concern." Prosser & Keeton on Torts § 44, at 318 (5th ed. 1984).

the criminal conduct. Other civil cases have gone the other way. See Herceg v. Hustler Magazine, Inc., 814 F.2d 1017 (5th Cir. 1987) (holding that publisher of article describing how to perform autoerotic asphyxia could not be civilly liable for inciting the death of a teenager).

In any event, no one contended that Hit Man's publisher might be criminally prosecuted.

Not so here, raising the concern voiced by the First Circuit in Czubinski:

> The broad language of the mail and wire fraud statutes are both their blessing and their curse. They can address new forms of serious crime that fail to fall within more specific legislation. On the other hand, they might be used to prosecute kinds of behavior that, albeit offensive to the morals or aesthetics of federal prosecutors, cannot reasonably be expected by the instigators to form the basis of a federal felony.

Czubinski, 106 F.3d at 1079 (citation omitted). The fact that the federal government pursued Harris criminally based on evolving, previously uncharged and uncriminalized conduct begs the constitutional question whether the wire fraud statute, with its soft boundaries and built-in ambiguities, gives fair notice of possible prosecution. Certainly, no large internet actor has reason to fear the statute's wooly terms might threaten prison for its corporate principals. Certainly, Sony never feared its VCR technology would generate a criminal infringement action. Nor would telephone providers who deliberately piggy-backed on competitor's phone lines for commercial advantage. Harris's own statements prior to his prosecution indicate that he never could have anticipated that making and selling a device with certain known capabilities would land him in criminal proceedings. As the back cover of the book states, use of these products to obtain free or faster service might get you in hot water with your ISP, but there is not a word warning or indicating that anyone could have foreseen federal criminal prosecution. Harris's

conversations similarly evince a concern that ISPs might come after the company or its assets, but show no recognition that TCNISO was, itself, a federal crime.

Using the criminal law as a battle ground, selectively and arbitrarily, to litigate Harris's responsibility as a firmware seller for product use by customers, as well as to delineate the boundaries of the definition of property and fraud in the ever-developing field of internet access, exceeds the bounds of the statute. In this context, the wire fraud statute is void for vagueness, and this Court should grant a judgment of acquittal or a new trial.

II. CONCLUSION

For the foregoing reasons, this Court should enter a judgment of acquittal as to all counts, as this application of the wire fraud statute is void for vagueness and violates Harris's Constitutional rights.

RYAN HARRIS
By his attorney,

/s/ Charles P. McGinty

Charles P. McGinty
B.B.O. #333480
Federal Defender Office
51 Sleeper Street
Boston, MA 02210
Tel: 617-223-8061

CERTIFICATE OF SERVICE

I hereby certify that this document, filed through the ECF system, will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to those indicated as non-registered participants on March 15, 2012.

/s/ Charles P. McGinty

Charles P. McGinty